IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

CHRIS UNDERWOOD, JESSICA PRESTON, HULOFTON ROBINSON, JESSICA AUSTIN, STEVEN CHECCHIA, JEANPAUL MAGALLANES, and DANA FOLEY on behalf of themselves and all others similarly situated, Plaintiffs, v. JERICO PICTURES, INC. d/b/a NATIONAL PUBLIC DATA, Defendant.	Case No. _____ JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Chris Underwood, Jessica Preston, Hulofton Robinson, Jessica Austin, Steven Checchia, JeanPaul Magallanes, and Dana Foley (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, assert the following against Defendant Jerico Pictures, Inc. d/b/a National Public Data ("NPD" or "Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

INTRODUCTION

1. Plaintiffs bring this class action complaint against Defendant for its (i) failure to properly secure and safeguard highly valuable, protected personally identifiable information, including without limitation, Plaintiffs' and Class Members' full names, Social Security numbers, phone numbers, mailing addresses and other personal information (collectively "PII"); (ii) failure to comply with industry standards to protect information systems that contain PII; (iii) unlawful

disclosure of Plaintiffs' and Class Members' PII; and (iv) failure to provide timely and adequate notice to Plaintiffs and other Class Members that their PII had been disclosed.

2. Defendant is a corporation providing data-related services, including background checks for its clients.

3. Defendant, on August 15, 2024, reported to regulators that in or around June 2024, Defendant experienced a breach impacting its systems, where a third-party bad actor gained entry to Defendant's computer networks and systems, accessed the PII and exfiltrated the information from those systems. Specifically, Defendant's disclosure stated that the company has experienced a "data security incident…believed to have involved a third-party bad actor" who tried to hack into its data in late December 2023, "with potential leaks of certain data in April 2024 and summer 2024" (i.e., the "Data Breach").

4. Defendant further stated that 1.3 million individuals were affected by the Data Breach in a breach notification published by the Office of the Maine Attorney General. It is also reported that the leaked PII includes 420 million distinct mailing addresses, 272 million distinct Social Security numbers, and over 160 million distinct phone numbers[1] that were accessed and stolen by an unauthorized third-party.

5. The Data Breach occurred as a result of Defendant's failures, including lax security protocols. These failures enabled cybercriminals to gain access to Defendant's systems and/or servers and exfiltrate the PII of potentially millions of individuals, including their full names, Social Security numbers, phone numbers, mailing addresses and other personal information. The exfiltrated PII remains in the hands of the cyber-criminals who seek to profit off the stolen PII by exploiting and stealing the identities of Plaintiffs and the Class Members.

[1] *See* https://spycloud.com/blog/national-public-data-breach-analysis/ (last accessed Sept. 12, 2024).

6. The Data Breach was a direct and proximate result of Defendant's flawed online system configuration and design and Defendant's failure to implement and follow basic security procedures.

7. Because of Defendant's failures, unauthorized individuals were able to access and pilfer Plaintiffs' and Class Members' PII. Plaintiffs' and Class Members' identities are now at risk due to Defendant's negligent conduct because the highly valuable PII that Defendant collected and maintained has been accessed and acquired by data thieves.

8. As a result, Plaintiffs and Class Members are at substantially increased risk of future identity theft, both currently and for the indefinite future. Plaintiffs' and Class Members' PII, including their Social Security numbers, that were compromised by cybercriminals in the Data Breach, is highly valuable because it is readily useable to commit fraud and identity theft. Plaintiffs and Class Members are at the peril of suffering financial risks, including but not limited to criminals opening new financial accounts in Plaintiffs' and Class Member's names, using the stolen PII to obtain governmental benefits, filing false tax returns, and obtaining driver's licenses.

9. Plaintiffs, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, breach of third-party beneficiary contract, unjust enrichment, the California Consumer Privacy Act, and California Customer Records Act.

10. Plaintiffs seeks damage and injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

11. Given that information relating to the Data Breach, including the systems that were impacted and the configuration and design of Defendant's website and systems, remain exclusively

in Defendant's control, Plaintiffs anticipate additional support for their claims will be uncovered following a reasonable opportunity for discovery.

JURISDICTION AND VENUE

12. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d)(2), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative Members of the Class defined below, and a significant portion of putative Class Members are citizens of a different state than Defendant.

13. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, Defendant is registered to do business in Florida and conducts substantial business in this District, and a substantial portion of the violations, acts, and omissions giving rise to this action occurred in this District.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District, Defendant does business in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

A. Plaintiffs

15. Plaintiff Chris Underwood ("Plaintiff Underwood") is a citizen and resident of the State of Florida. On September 12, 2024, Plaintiff Underwood received an Experian IdentityWorks alert that his Social Security number was on the dark web. This alert identified the "National Public Data" Data Breach as the likely source from which his Social Security number was taken.

16. A website set-up for those affected by the NPD Data Breach has confirmed that Plaintiff Underwood's PII (including his name, address, phone number, and social security

number) was compromised in the breach. While Plaintiff Underwood is not a customer of Defendant, Defendant may have conducted a background check for a previous employer or his PII may have been scraped from non-public sources by the Defendant.

17. Plaintiff Hulofton Robinson ("Plaintiff Robinson") is a citizen and resident of the State of California. Following news of the NPD Data Breach, Plaintiff Robinson visited the website set-up for those affected by the NPD Data Breach and confirmed that his PII (including his name, address, phone number, and social security number) was compromised in the breach. While Plaintiff Robinson is not a customer of Defendant, Defendant may have conducted a background check for a previous employer or his PII may have been scraped from non-public sources by the Defendant.

18. Plaintiff Jessica Preston ("Plaintiff Preston") is a citizen and resident of the State of New York. Following news of the NPD Data Breach, Plaintiff Preston visited the website set-up for those affected by the NPD Data Breach and confirmed that her PII (including her name, address, phone number, and social security number) was compromised in the breach. While Plaintiff Robinson is not a customer of Defendant, Defendant may have conducted a background check for a previous employer or her PII may have been scraped from non-public sources by the Defendant.

19. Plaintiff Jessica Austin ("Plaintiff Austin") is a citizen and resident of the State of Florida. Following news of the NPD Data Breach, Plaintiff Austin visited the website set-up for those affected by the NPD Data Breach and confirmed that her PII (including her name, address, phone number, and social security number) was compromised in the breach. While Plaintiff Austin is not a customer of Defendant, Defendant may have conducted a background check for a previous employer or her PII may have been scraped from non-public sources by the Defendant.

20. Plaintiff Dana Foley ("Plaintiff Foley") is a citizen and resident of the State of Illinois. On August 24, 2024, Plaintiff Foley received a Dark Web Monitoring Alert from Identity Defense notifying Plaintiff Foley that Plaintiff Foley's social security number had been found on the dark web. While Plaintiff Foley is not a customer of Defendant, Defendant may have conducted a background check for a previous employer or Plaintiff Foley's PII may have been scraped from non-public sources by the Defendant.

21. Plaintiff JeanPaul Magallanes ("Plaintiff Magallanes") is a citizen and resident of the State of Nevada. On September 6, 2024, Plaintiff Magallanes was notified via a dark web monitoring service that his Social Security Number had been found on the dark web. Following this alert, Plaintiff Magallanes visited the website set-up for those affected by the NPD Data Breach and confirmed that Plaintiff Magallanes's PII (including name, address, phone number, and social security number) was compromised in the breach. While Plaintiff Magallanes is not a customer of Defendant, Defendant may have conducted a background check for a previous employer or Plaintiff Magallanes's PII may have been scraped from non-public sources by the Defendant.

22. Plaintiff Steve Checchia ("Plaintiff Checchia") is a citizen and resident of the Commonwealth of Pennsylvania. On August 11, 2024 a dark web monitoring service identified Plaintiff Checchia's Social Security Number on the dark web. Following this alert, Plaintiff Checchia visited the website set-up for those affected by the NPD Data Breach and confirmed that Plaintiff Checchia's PII (including name, address, phone number, and social security number) was compromised in the breach. While Plaintiff Checchia is not a customer of Defendant, Defendant may have conducted a background check for a previous employer or Plaintiff Checchia's PII may have been scraped from non-public sources by the Defendant.

B. Defendant

23. Defendant Jerico Pictures Inc. d/b/a National Public Data is a corporation organized under the state laws of Florida with its headquarters and principal place of business located at 1801 NW 126th Way, Coral Springs, Florida 33071.

24. Defendant is a corporation that provides data-related services, including running background checks and providing person lookup and verification tools for many different businesses. Defendant's services are used by private investigators, consumer public record sites, human resources professionals, staffing agencies, and others. As part of its business, the Defendant collects valuable PII from its client's customers, such as Plaintiffs and the Class Members.

BACKGROUND

I. Defendant Obtains, Collects, and Stores PII

25. Defendant is in complete operation, control, and supervision of its systems, and configured and designed its systems without adequate data security protections.

26. Defendant was entrusted with safely securing and safeguarding Plaintiffs' and Class Members' PII.

27. Defendant did not properly verify, oversee, and supervise its entrustment of Plaintiffs' and Class Members' PII. The information held by Defendant included unencrypted PII, a bulk of which was collected from Class Members via background checks under the impression that the submitted information would be kept safe, confidential and private.

28. By obtaining, using, disclosing, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

29. Plaintiffs and Class Members reasonably expect that a massive data company like Defendant, who is entrusted with highly confidential information, will use the utmost care to keep

their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. Despite the sensitive nature of Defendant's business, Defendant failed to prioritize data and cybersecurity by adopting reasonable data and cybersecurity measures to prevent and detect the unauthorized access to Plaintiffs' and Class Members' PII.

31. Had Defendant followed industry guidelines and adopted reasonable security measures, Defendant would have prevented intrusion into its information systems and, ultimately, the theft of Plaintiffs' and Class Members' PII.

II. FTC Guidelines

32. Defendant is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

33. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

34. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

35. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII, or to prevent the disclosure of such information to unauthorized individuals, as reflected by the sensitive Social Security information and other PII stolen, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

38. Defendant was always fully aware of its obligations to protect the PII of consumers because of its business of obtaining, collecting, and disclosing PII as well as collecting, storing, and using other confidential personal and financial information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

SUBSTANTIVE ALLEGATIONS

I. The Data Breach

39. On or no later than April 2024, Plaintiffs' and Class Members' sensitive PII was compromised. Through a post on its website on or around August 15, 2024, Defendant announced that "a data security incident…believed to have involved a third-party bad actor" who tried to hack into its data in late December 2023 occurred, "with potential leaks of certain data in April 2024

and summer 2024," allowing an unauthorized third-party to access Defendant's computer systems, which stored unencrypted PII of Plaintiffs and Class Members, including their full names, addresses, Social Security numbers, phone numbers, and other personal information (the "Data Breach").

40. Subsequently, the cybercriminal group USDoD took credit for the Data Breach and "put the database up for sale for $3.5 million on an underworld forum in April, and rather incredibly claimed the trove included 2.9 billion records on all US, Canadian, and British citizens."[2]

41. Despite that the Data Breach occurred no later than April 2024, the Defendant waited until at least August 10, 2024, to provide *any* notice to the affected individuals, according to the breach notification published by the Office of the Maine Attorney General. On August 10, 2024, when Defendant began notifying affected individuals, its notice stated:

What Happened?

> There appears to have been a data security incident that may have involved some of your personal information. The incident is believed to have involved a third-party bad actor that was trying to hack into data in late December 2023, with potential leaks of certain data in April 2024 and summer 2024. We conducted an investigation and subsequent information has come to light. What Information Was Involved? The information that was suspected of being breached contained name, email address, phone number, social security number, and mailing address(es).

What We Are Doing

> We cooperated with law enforcement and governmental investigators and conducted a review of the potentially affected records and will try to notify you if there are further significant developments applicable to you. We have also implemented

[2] https://www.theregister.com/2024/06/03/usdod_data_dump/

> additional security measures in efforts to prevent the reoccurrence of such a breach and to protect our systems.

42. Defendant admitted that an unauthorized third-party bad actor accessed its network systems containing the sensitive PII. The stolen information included, without limitation, full names, addresses, Social Security numbers, and phone numbers. The information also included details about an individual's parents, siblings, and other relatives, such as aunts, uncles, and cousins, both alive and deceased.

43. Plaintiffs' PII was disclosed without their authorization to unknown third parties as a result of the Data Breach.

44. As a result of the Data Breach, Plaintiffs spent time and effort researching the Data Breach, reviewing and monitoring their accounts for fraudulent activity, reviewing credit monitoring services, and dealing with phishing attempts via email and telephone calls using the information taken in the Data Breach.

45. For example, Plaintiff Underwood received an alert that his social security number was found on the dark web following the NPD Data Breach. He spent time researching the Data Breach to confirm that his PII had been compromised in the Data Breach.

46. Similarly, Plaintiff Robinson discovered fraudulent purchases on one of his accounts following the Data Breach and had to contact his bank and replace his debit card. After this incident, Plaintiff Robinson verified that his PII had been compromised in the Data Breach.

47. The Data Breach has caused the Plaintiffs to suffer anxiety and stress from concerns that they face an increased risk of financial fraud, identity theft and other types of monetary harm as a result of the stolen information. Plaintiffs place significant value in the security of their PII.

48. Plaintiffs and Class Members suffered actual damages as a result of the failures of Defendant to adequately protect the sensitive information entrusted to it, including, without

limitation, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their PII, and other economic and non-economic harm. Plaintiffs and Class Members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

49. As a result of the Data Breach, Plaintiffs have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach. As mentioned above, they also continue to suffer from anxiety and fear of financial fraud and identity theft.

II. Defendant's Data Security Failures Caused the Data Breach

50. Up to, and including, the period when the Data Breach occurred, Defendant breached its duties, obligations, and promises to Plaintiffs and Class Members, by its failure to:

a. hire qualified personnel and maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. properly train its employees about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, what to do if they suspect such attacks, and how to prevent them;

c. address well-known warnings that its systems and servers were susceptible to a data breach;

d. implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its systems that accessed individual's

personal information and otherwise would have protected their sensitive personal information;

e. install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented individual's sensitive PII from being stolen. Specifically, there are recommended, available measures to prevent data from leaving protected systems and being sent to untrusted networks outside of the corporate systems; and

f. adequately safeguard individual's sensitive PII and maintain an adequate data security environment to reduce the risk of a data breach or unauthorized disclosure.

III. Defendant's Data Security Failures Constitute Unfair and Deceptive Practices and Violations of Consumers' Privacy Rights

51. The FTC deems the failure to employ reasonable and appropriate measures to protect against unauthorized access to sensitive personal information an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

53. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

54. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure sensitive personal information. These orders provide further guidance to businesses regarding their data security obligations.

55. Prior to the Data Breach, and during the breach itself, Defendant failed to follow guidelines set forth by the FTC and actively mishandled the management of its IT security.

56. Furthermore, by failing to have reasonable data security measures in place, Defendant engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

IV. The Value of the Disclosed PII and Effects of Unauthorized Disclosure

57. Defendant understood the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

58. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers.

59. Sensitive personal information commonly stolen in data breaches has economic value. The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information.

60. The forms of PII involved in this Data Breach are particularly concerning. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

61. The Social Security Administration (''SSA") warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

62. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security

numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

63. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe.

64. To avoid detection, identity thieves often hold stolen data for months or years before using it. The stolen PII is freely available on the dark web and thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

65. Thus, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

66. As a highly sophisticated entity that handles sensitive PII, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

67. Identity thieves use stolen PII for various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud and government fraud.

68. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through

unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

69. There is often a lag time between when fraud occurs versus when it is discovered, and also between when PII is stolen and when it is used.

70. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

71. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years.

72. Plaintiffs and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

73. Thus, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

V. The Data Breach Damaged Plaintiffs and Class Members

74. According to research, sensitive PII can sell for as much as $363 per record.[3] As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to

[3] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing additional loss of value.

75. As a result of Defendant's deficient security measures, Plaintiffs and Class Members are also under a constant threat of their PII being used by criminals for identify theft and other fraud-related crimes.

76. Plaintiffs and Class Members face a substantial and imminent risk of fraud and identity theft as their names have now been linked with their Social Security numbers, emails, phone numbers, and physical addresses as a result of the Data Breach. These specific types of information are associated with a high risk of fraud.

77. As an example of this risk of fraud, Plaintiff Underwood received an alert that his Social Security number was found on the dark web, which he learned had been disclosed in the NPD Data Breach. Similarly, Plaintiff Robinson discovered fraudulent purchases in one of his accounts following the Data Breach and had to contact his bank and replace his debit card.

78. Many Class Members will also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

79. Plaintiffs and Class Members also suffered a "loss of value" of their sensitive PII when it was stolen by hackers in the Data Breach. A robust market exists for stolen PII. Hackers sell PII on the dark web—an underground market for illicit activity, including the purchase of hacked PII—at specific identifiable prices. This market serves as a means to determine the loss of value to Plaintiffs and Class Members. Here, the hackers already tried to sell the data for $3.5 million on the dark web, which has since been released for free.

80. Identity thieves can also combine data stolen in the Data Breach with other information about Plaintiffs and Class Members gathered from underground sources, public sources, or even Plaintiffs' and Class Members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiffs and Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members' information, obtaining Social Security numbers in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

81. Plaintiffs and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud andthe opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. These efforts are burdensome and time-consuming, especially because Defendant has disclosed little information about the Data Breach, forcing customers to continue to monitor their accounts indefinitely.

82. Plaintiffs and Class Members who experience identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will be harmed further by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans,

late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

83. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again, especially when that individual spent significant time monitoring their accounts and rectifying any problems that arose.

84. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information (including Social Security number) has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

85. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. The stolen PII is freely available on the dark web which may be used at any time by the bad actors, including after many months or more to target Plaintiffs and the Class Members. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

VI. Defendant's Failure to Timely Notify Plaintiffs and Class Members

86. As detailed above, the Data Breach occurred no later than April 2024 (and was ongoing since December 2023). Defendant claims to have discovered the Data Breach in August 2024, and only began notifying Plaintiffs and Class Members of the Data Breach on or around August 10, 2024.

87. Defendant's failure to realize that its systems had been compromised resulted in a squandering of time. This is time that could have been used by Plaintiffs and Class Members to take steps to mitigate the damage caused by the Data Breach.

88. Instead, Defendant concealed the Data Breach for more than two weeks and potentially four months, allowing the unauthorized third-party to potentially exploit Plaintiffs' and Class Members' PII without any mitigation steps being taken.

89. Plaintiffs and Class Members were deprived of the opportunity to take any steps to prevent damage by Defendant's concealment of the Data Breach and failure to provide timely and adequate notice of the Data Breach to Plaintiffs and Class Members.

CLASS ACTION ALLEGATIONS

90. Plaintiffs brings this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Nationwide Class:

> All persons in the United States whose PII was compromised in the Data Breach made public by Jerico Pictures Inc. d/b/a National Public Data in August 2024 (the "Nationwide Class").

91. Excluded from the Class are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

92. Plaintiffs reserve the right to modify, expand or amend the above Class definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

93. Plaintiffs also bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following California Subclass:

> All persons in California whose PII was compromised in the Data Breach made public by Jerico Pictures Inc. d/b/a National Public Data in August 2024 (the "California Subclass").

94. Excluded from the California Subclass are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

95. Plaintiffs reserve the right to modify, expand or amend the above California Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

96. Plaintiffs also bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Illinois Subclass:

> All persons in Illinois whose PII was compromised in the Data Breach made public by Jerico Pictures Inc. d/b/a National Public Data in August 2024 (the "Illinois Subclass").

97. Excluded from the Illinois Subclass are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

98. Plaintiffs reserve the right to modify, expand or amend the above Illinois Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

99. Plaintiffs also bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2) and (b)(3) on behalf of the following Nevada Subclass:

> All persons in Nevada whose PII was compromised in the Data Breach made public by Jerico Pictures Inc. d/b/a National Public Data in August 2024 (the "Nevada Subclass").

100. Excluded from the Nevada Subclass are Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

101. Plaintiffs reserve the right to modify, expand or amend the above Nevada Subclass definition or to seek certification of a class or classes defined differently than above before any court determines whether certification is appropriate following discovery.

102. Certification of Plaintiffs' claims for class-wide treatment are appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

103. **Numerosity**. All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The Members of the Class are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. There are likely millions of Members of the Class. In a breach notification published by the Office of the Maine Attorney General, Defendant said 1.3 million individuals were affected by the Data Breach. It is also reported that the leaked PII includes 420 million distinct mailing addresses, 272 million distinct Social Security numbers, and over 160

million distinct phone numbers[4] that were accessed and stolen by an unauthorized third-party. Although, the precise number of Class Members is unknown to Plaintiffs.

104. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

105. **Commonality and Predominance**. All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members, including, without limitation:

a. Whether Defendant engaged in active misfeasance and misconduct alleged herein;

b. Whether Defendant owed a duty to Class Members to safeguard their sensitive PII;

c. Whether Defendant breached its duty to Class Members to safeguard their sensitive PII;

d. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

e. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of the Data Breach;

f. Whether Defendant's failure to provide adequate security proximately caused Plaintiffs' and Class Members' injuries; and

g. Whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief.

106. **Typicality.** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of all Class Members because Plaintiffs, like other Class Members, suffered theft of their sensitive personal information in the Data Breach.

[4] *See* https://spycloud.com/blog/national-public-data-breach-analysis/ (last accessed Sept. 12, 2024)

107. **Adequacy of Representation.** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiffs are an adequate Class representative because they are a Member of the Class and their interests do not conflict with the interests of other Class Members that they seek to represent. Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interest in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

108. **Predominance and Superiority.** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiffs' case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Members of the Class to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

109. **Cohesiveness**. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant has acted, or refused to act, on grounds generally applicable to the Class such that final declaratory or injunctive relief is appropriate.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of All Plaintiffs and the Nationwide Class)

110. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein.

111. Defendant obtained Plaintiffs' and Class Members' PII. Upon information and belief, Defendant scrapes the PII of individuals, including Plaintiffs and Class Members, in the ordinary course of providing background check services to its clients. Defendant scrapes the PII of individuals from non-public sources, including but not limited to, its clients. Plaintiffs and Class Members also entrusted their PII to Defendant's non-public clients, and Defendant scraped and then stored this PII for the purpose of providing background check services for a profit.

112. By collecting and maintaining sensitive PII, Defendant had a common law duty of care to use reasonable means to secure and safeguard the sensitive personal information and to prevent disclosure of the information to unauthorized individuals. Defendant's duty included a responsibility to implement processes by which it could detect a data breach of this type and magnitude in a timely manner.

113. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with the various statutory requirements, regulations, and other notices described above.

114. Defendant was subject to an "independent duty" untethered to any contract between Plaintiffs and Class Members and Defendant.

115. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' valuable and sensitive PII.

116. Defendant's negligent acts and omissions include, but are not limited to, the following:

a. failure to employ systems and educate employees to protect against malware;

b. failure to comply with industry standards for software and server security;

c. failure to track and monitor access to its network;

d. failure to limit access to those with a valid purpose;

e. failure to adequately staff and fund its data security operation;

f. failure to remove, delete, or destroy highly sensitive personal information of individuals that is no longer being used for any valid business purpose;

g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

h. failure to recognize that hackers were stealing PII from its network while the Data Breach was taking place; and

i. failure to oversee the entrustment of PII.

117. It was foreseeable to Defendant that a failure to use reasonable measures to protect its customers' sensitive PII could result in injury to its clients, Plaintiffs and Class Members. Further, actual and attempted breaches of data security were reasonably foreseeable to Defendant given the known frequency of data breaches and various warnings from industry experts.

118. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured as alleged herein. Plaintiffs and Class Members are entitled to

damages, including actual, compensatory, punitive, and nominal damages suffered because of the Data Breach in an amount to be proven at trial.

119. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of All Plaintiffs and the Nationwide Class)

120. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein.

121. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect sensitive PII.

122. Various FTC publications and orders also form the basis of Defendant's duty.

123. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

124. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

125. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against

businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

126. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured as alleged herein. Plaintiffs and Class Members are entitled to damages, including actual, compensatory, punitive, and nominal damages suffered because of the Data Breach in an amount to be proven at trial.

127. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

128. Plaintiffs' and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of All Plaintiffs and the Nationwide Class)

129. Plaintiffs re-allege and incorporates by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein.

130. Defendant entered into written contracts, including with its clients to provide data services including background checks and person lookup.

131. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiffs and the Class and to timely and adequately notify them of the Data Breach. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, then its clients' customers—Plaintiffs and Class Members—would be harmed.

132. Upon information and belief, Plaintiffs and Class Members were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current customers, that upon information and belief, include obligations to protect, safeguard, and keep secure the PII of Plaintiffs and Class Members.

133. Defendant's representations required Defendant to implement the necessary security measures to safeguard the PII of Plaintiffs and Class Members and not take unjustified risks when storing the PII.

134. Defendant materially breached its contractual obligation to protect the PII of Plaintiffs and Class Members when the information was accessed and exfiltrated by an unauthorized third party as a result of the Data Breach. Defendant breached its contractual obligation by failing to safeguard and protect Plaintiffs' and Class Members' PII and by failing to provide accurate and prompt notice to them that their PII was compromised as a result of the Data Breach. Defendant further breached its contractual obligation by failing to (i) encrypt or tokenize the sensitive PII of Plaintiffs and Class Members, (ii) delete such PII that Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

135. Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

136. Plaintiffs and Class Members were harmed by Defendant's conduct as a direct and proximate result of Defendant's breach of its contracts with its clients and are entitled to the damages they have sustained. Plaintiffs and Class Members are entitled to damages, including

actual, compensatory, punitive, and nominal damages suffered because of the Data Breach in an amount to be proven at trial.

137. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On behalf of All Plaintiffs and the Nationwide Class)

138. Plaintiffs re-allege and incorporates by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein.

139. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of PII, and in same cases paid monies to Defendant's clients who used Defendant's background check services.

140. Defendant accepted or knew that Plaintiffs and Class Members conferred a monetary benefit to Defendant's customers, and thereby Defendant, and accepted and retained those benefits by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs' and Class Members' retained data and used Plaintiffs' and Class Members' PII for business purposes.

141. The monies paid to Defendant were supposed to be used by Defendant, in part, to pay for and oversee adequate data privacy infrastructure, practices, and procedures.

142. In equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to oversee, implement, or adequately implement, the data privacy and security practices and procedures that

Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

143. As a result of Defendant's conduct, Plaintiffs and Class Members have been injured as alleged herein.

144. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

145. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pled.

COUNT V
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code §§ 1798.150, *et seq.*
(On behalf of Plaintiff Robinson and the California Subclass)

146. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein.

147. Plaintiff Robinson is a resident of California.

148. Upon information and belief Defendant is a business under Cal. Civ. Code § 1798.140(d).

149. Defendant purposefully does business with California entities and purposefully collects data concerning California citizens in furtherance of its data business, which includes background check service and data brokering.

150. Defendant collects consumers' personal information ("PII" for purposes of this Count) as defined in Cal. Civ. Code § 1798.140.

151. Defendant violated § 1798.150 of the CCPA by failing to protect Plaintiff Robinson's and California Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

152. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Robinson's and California Subclass Members' PII. As detailed herein, Defendant failed to do so.

153. As a direct and proximate result of Defendant's acts, the PII of Plaintiff Robinson and California Subclass Members, including Social Security numbers were subjected to unauthorized access and exfiltration, theft, or disclosure.

154. Plaintiff Robinson and California Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including Plaintiff Robinson's and California Members' PII. Plaintiff Robinson and California Subclass Members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

155. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

156. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

157. Plaintiff Robinson and the California Subclass will ultimately seek statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

158. Plaintiff Robinson will send the appropriate CCPA notice letters to Defendant providing the notice required by Cal. Civ. Code § 1798.150(b) and will amend their claim to assert claims for damages against Defendant.

COUNT VI
CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")
Cal. Civ. Code §§ 1798.80, *et seq.*
(On behalf of Plaintiff Robinson and the California Subclass)

159. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein.

160. Plaintiff Robinson is a resident of California.

161. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure."

162. Defendant is a business that owns, maintains, and licenses personal information (or "PII"), within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff Robinson and California Subclass Members.

163. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of PII that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

164. Defendant is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

165. Plaintiff Robinson's and California Subclass Members' PII (e.g., Social Security numbers) includes PII as covered by Cal. Civ. Code § 1798.82.

166. Because Defendant reasonably believed that Plaintiff Robinson's and California Subclass Members' PII was acquired by unauthorized persons during the Defendant's Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

167. Defendant failed to fully disclose material information about the Data Breach, including the types of PII impacted, in a timely fashion.

168. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

169. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Robinson and California Subclass Members suffered damages, as described above.

170. Plaintiff Robinson and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT VII
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
l. Comp. Stat. §§ 510/2, *et seq.*
(On behalf of Plaintiff Foley and the Illinois Subclass)

171. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein

172. Defendant is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

173. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including by failing to protect Plaintiff Foley's and Illinois Subclass members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

174. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Foley's and Illinois Subclass members' PII. As detailed herein, Defendant failed to do so.

175. As a direct and proximate result of Defendant's acts, the PII of Plaintiff Foley and Illinois Subclass members, including Social Security numbers were subjected to unauthorized access and exfiltration, theft, or disclosure.

176. Plaintiff Foley and Illinois Subclass members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing

reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including Plaintiff Foley's and Illinois Subclass members' PII. Plaintiff Foley and Illinois Subclass members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

177. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Foley and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

178. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive trade practices, Plaintiff Foley and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

179. Plaintiff Foley and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT VIII

NEVADA DECEPTIVE TRADE PRACTICES ACT, Nev. Rev. Stat. Ann. §§ 598.0903, et seq. (On behalf of Plaintiff Magallanes and the Nevada Subclass)

180. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 109, as if fully set forth herein.

181. Defendant advertised, offered, or sold goods or services in Nevada and engaged in trade or commerce directly or indirectly affecting the people of Nevada.

182. Defendant engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including by failing to protect Plaintiff Magallanes's and Nevada Subclass members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

183. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Magallanes's and Nevada Subclass members' PII. As detailed herein, Defendant failed to do so.

184. As a direct and proximate result of Defendant's acts, the PII of Plaintiff Magallanes's and Nevada Subclass members, including Social Security numbers were subjected to unauthorized access and exfiltration, theft, or disclosure.

185. Plaintiff Magallanes's and Nevada Subclass members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including Plaintiff Magallanes's and Nevada Subclass members' PII. Plaintiff Magallanes's and Nevada Subclass members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

186. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff Magallanes and Nevada Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

187. Plaintiff Magallanes and Nevada Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

COUNT IX
DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of All Plaintiffs and the Nationwide Class)

188. Plaintiffs re-allege and incorporate by reference all of the allegations contained in paragraphs 1 through 99, as if fully set forth herein.

189. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

190. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and statutory duties to reasonably safeguard Plaintiffs' and Class Members' sensitive PII and whether Defendant is currently maintaining data

security measures adequate to protect Plaintiffs and Class Members from further data breaches. Plaintiffs allege that Defendant's data security practices remain inadequate.

191. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their sensitive PII and remain at imminent risk that further compromises of their PII will occur in the future.

192. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure Plaintiffs' and Class Members' sensitive PII, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure Plaintiffs' and Class Members' sensitive PII.

193. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive PII.

194. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law, because not all of the resulting injuries are readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

195. The hardship to Plaintiffs and Class Members if an injunction does not issue greatly exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Defendant of complying with an injunction by employing

reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

196. Issuance of the requested injunction will serve the public interest by preventing another data breach at NPD, thus eliminating the additional injuries that would result to Plaintiffs and the millions of individuals whose confidential information would be further compromised.

REQUEST FOR RELIEF

Plaintiffs, on behalf of all others similarly situated, request that the Court enter judgment against Defendant including the following:

A. Determining that this matter may proceed as a class action and certifying the Class asserted herein;

B. Appointing Plaintiffs as representatives of the applicable Class and Subclass and appointing Plaintiffs' counsel as Class Counsel;

C. An award to Plaintiffs and the Classes of damages, including actual, compensatory, punitive, and nominal damages as set forth above;

D. Disgorgement into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by NPD as a result of the conduct and Data Breach as set forth above;

E. Ordering injunctive relief requiring Defendant to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; (iii) provide several years of free credit monitoring and identity theft insurance to all Class Members; and (iv) timely notify individuals of any future data breaches;

F. Entering a declaratory judgment stating that Defendant owes a legal duty to secure Plaintiffs' and Class Members' sensitive PII, to timely notify its clients and any person or business

entity of any data breach, and to establish and implement data security measures that are adequate to secure sensitive personal information;

G. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

H. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

I. Such other relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: September 17, 2024

Respectfully submitted,

/s/ Michelle C. Clerkin
Michelle C. Clerkin
Florida Bar No. 1045076
SPIRO HARRISON & NELSON
1111 Lincoln Road, Suite 500
Miami Beach, FL 33139
Tel.: (786) 841-1181
mclerkin@shnlegal.com

Christian Levis (pro hac vice filed simultaneously with this complaint)
Peter Demato (pro hac vice filed simultaneously with this complaint)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel.: (914) 997-0500
clevis@lowey.com
pdemato@lowey.com

Anthony M. Christina (pro hac vice filed simultaneously with this complaint)
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428

Tel: (215) 399-4770
achristina@lowey.com

Ian W. Sloss (pro hac vice filed simultaneously with this complaint)
Johnathan Seredynski (pro hac vice filed simultaneously with this complaint)
SILVER GOLUB & TEITELL LLP
One Landmark Square, Floor 15
Stamford, CT 06901
Tel.: (203) 325-4491
isloss@sgtlaw.com
jseredynski@sgtlaw.com

Counsel for Plaintiffs Chris Underwood, Jessica Preston, Hulofton Robinson, Jessica Austin, and the Proposed Classes